3 elementos imprescindibles en tu plan de respuesta a incidentes

Planifica una respuesta integral a incidentes antes de que surjan

Gartner

Prepárate para reaccionar con rapidez durante un incidente

La posibilidad de sufrir un incidente de ciberseguridad es una certeza, no una probabilidad. La cuestión es “cuándo”. La cobertura de estos incidentes en los medios de comunicación es cada vez más negativa, y tanto auditores como reguladores y otras partes interesadas esperan que las organizaciones cuenten con planes de gestión claros para minimizar el impacto en la marca, la reputación, el personal, los clientes y los accionistas.

Es indispensable que los directores de seguridad y gestión del riesgo se preparen. Las principales herramientas de preparación son un plan de respuesta documentado y un manual de estrategia detallado para cada incidente.

Esta guía contiene extractos de páginas de las herramientas y los manuales de estrategia de Gartner.* Todos los datos son ilustrativos.

* Las herramientas completas están disponibles si eres cliente de Gartner: Manual: Plan de respuesta a incidentes de ciberseguridad, Manual: Crea un manual para el ransomware y Manual: Ejercicio de simulación para preparar tu respuesta a ciberataques. Si eres cliente, puedes descargar las plantillas, personalizarlas y enviarlas a Gartner para su revisión por parte de expertos, que también responderán a las preguntas que tengas mientras desarrollas el plan.

Los pagos por ransomware superaron los **1.000 millones de euros** en 2023, un máximo histórico.

El 24 % de los incidentes de ciberseguridad tuvieron que ver con ransomware.

Fuente: The Chainalysis 2024 Crypto Crime Report; Cost of data breach, IBM 2023

Los 3 componentes que debes incluir

01

Crea un plan de respuesta a incidentes

Un plan general de respuesta a ciberincidentes

El coste medio de una filtración de datos alcanzó un máximo histórico en 2023: **4,45 millones de euros**. Esto representa un aumento del 2,3 % con respecto al coste de 2022, de 4,35 millones de euros. Desde una perspectiva a largo plazo, el coste medio ha aumentado un 15,3 % desde los 3,86 millones de euros del informe de 2020.

Fuente: IBM Cost of a Data Breach Report, 2023

02

Desarrolla manuales con respuestas detalladas

Guías detalladas para abordar escenarios de incidentes específicos

En 2023, el **51 %** de las organizaciones de todo el mundo carecían de un plan de respuesta a incidentes de ransomware.

Fuente: 2023 Thales Data Threat Report

03

Lleva a cabo ejercicios de simulación de respuesta

Pruebas periódicas para practicar los planes de respuesta a incidentes

El **10 %** de las organizaciones fueron objeto de intentos de ataques de ransomware en 2023.

Fuente: Check Point Research: 2023 — The year of Mega Ransomware attacks with unprecedented impact on global organizations

Los 3 componentes que debes incluir

01

Crea un plan de respuesta a incidentes

Un plan general de respuesta a ciberincidentes

02

Desarrolla manuales con respuestas detalladas

Guías detalladas para abordar escenarios de incidentes específicos

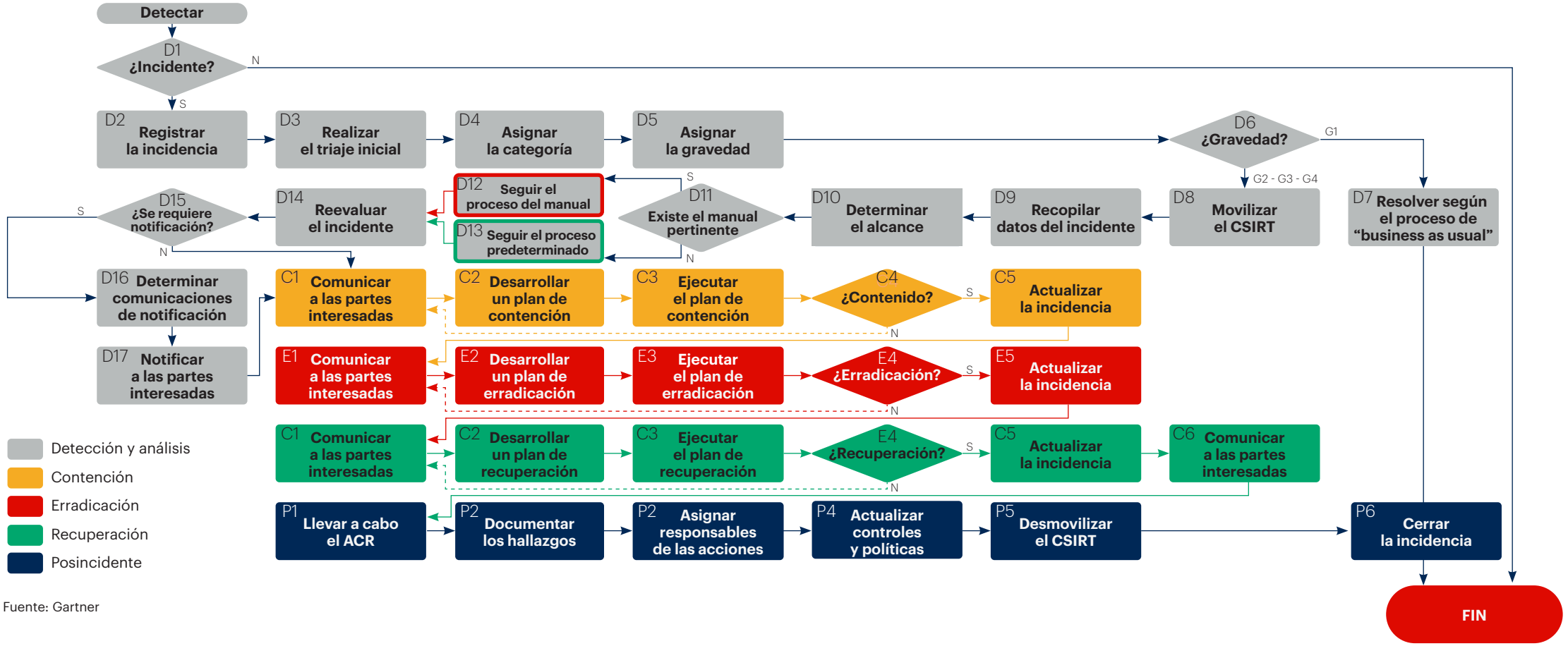
03

Lleva a cabo ejercicios de simulación de respuesta

Pruebas periódicas para practicar los planes de respuesta a incidentes

Crea un mapa del proceso de respuesta

El plan de respuesta a incidentes debe establecer unos pasos detallados para seguirlos secuencialmente en caso de incidentes. El coordinador de incidentes (o un puesto similar) garantizará que se sigan todos los pasos del proceso, hará un seguimiento del progreso y mantendrá una comunicación constante.



Fuente: Gartner

Define los niveles de gravedad del incidente

Todos los incidentes de seguridad deben clasificarse para asignarse a un nivel de gravedad. Esto sirve de guía al escalar los incidentes, asignar acuerdos de nivel de servicio e informar a las partes interesadas sobre el impacto potencial o real para la organización.

Gravedad	Impacto para la empresa					Atributos técnicos		
Nivel	Seguridad	Área legal	Privacidad	Finanzas	Reputación	Clase de datos	Volumen de datos	Operaciones
04 Crisis	Lesiones graves/ muerte	Impacto significativo	Multas: +Z euros	Pérdidas: +Z euros	Medios de comunicación mundiales	Ultrasecretos	A registros	Interrupción catastrófica
03 Alto	Lesiones graves	Impacto moderado	Multas: de Y euros a Z euros	Pérdidas: de Y euros a Z euros	Medios de comunicación nacionales	Secretos	Z registros	Interrupción grave
02 Medio	Primeros auxilios	Impacto bajo	Multas: de X euros a Y euros	Pérdidas: de X euros a Y euros	Medios de comunicación locales	Internos	Y registros	Interrupción menor
01 Bajo	Sin lesiones	Sin impacto	Sin infracciones	Sin pérdidas	Sin daños	Públicos	X registros	Sin interrupción

Fuente: Gartner

Define vías de escalado

Responder de forma eficaz a los incidentes se parece a practicar un deporte de equipo. Define unas vías de escalado claras basadas en la gravedad del incidente.

Gravedad	Vía de escalado					
Nivel	**Nota: El proceso de escalado es acumulativo a medida que aumenta el nivel de gravedad.**					
04 **Crisis**	CEO	CFO	Consejo de Administración	–	–	–
03 **Alto**	RR. HH.	Área Legal	COO	Privacidad	RR. PP.	Seguro de ciberseguridad
02 **Medio**	CISO	CIO	–	–	–	–
01 **Bajo**	Gestor de incidentes	CSIRT	–	–	–	–

Fuente: Gartner

Los 3 componentes que debes incluir

01

Crea un plan de respuesta a incidentes

Un plan general de respuesta a ciberincidentes

02

Desarrolla manuales con respuestas detalladas

Guías detalladas para abordar escenarios de incidentes específicos

03

Lleva a cabo ejercicios de simulación de respuesta

Pruebas periódicas para practicar los planes de respuesta a incidentes

Crea manuales de respuesta a incidentes

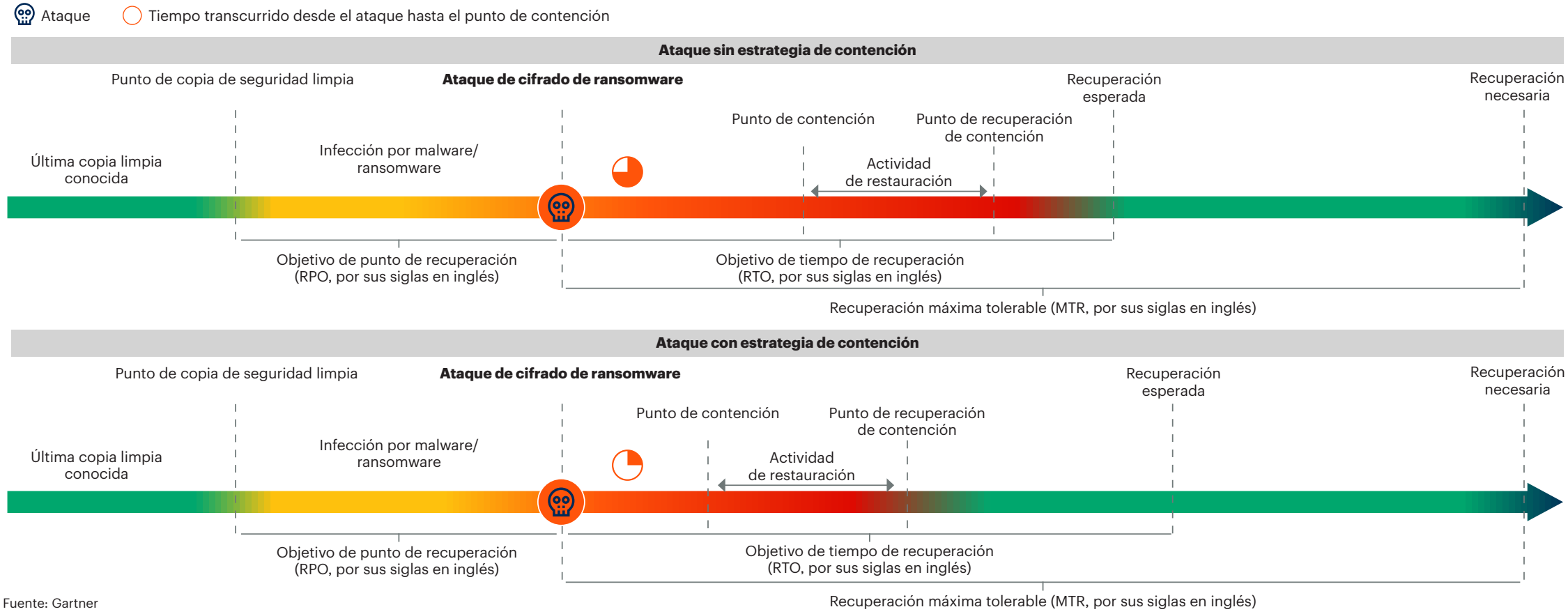
El equipo de respuesta a incidentes de ciberseguridad (CSIRT, por sus siglas en inglés) debe crear manuales específicos para los tipos de incidentes comunes o de mayor impacto, como los ataques de ransomware, según se ilustra en este ejemplo. Los manuales de respuesta están diseñados para proporcionar orientación y procedimientos más detallados que el plan general frente a los incidentes de seguridad.

Contenido

Fuente: Gartner

Desarrolla un flujo de trabajo de contención

Para reforzar la resiliencia de una organización durante un ataque de ransomware, los CISO deben trabajar con las partes interesadas en el desarrollo de una estrategia de contención. El objetivo clave de esta estrategia es minimizar el tiempo que transcurre desde el ataque hasta el punto de contención, además de limitar la disrupción para la empresa.



Fuente: Gartner

Los 3 componentes que debes incluir

01

Crea un plan de respuesta a incidentes

Un plan general de respuesta a ciberincidentes

02

Desarrolla manuales con respuestas detalladas

Guías detalladas para abordar escenarios de incidentes específicos

03

Lleva a cabo ejercicios de simulación de respuesta

Pruebas periódicas para practicar los planes de respuesta a incidentes

Crea un orden del día e invita a los participantes

En los ejercicios de simulación de respuesta a incidentes deben participar directivos y responsables de la toma de decisiones de toda la organización. Un buen ejercicio de simulación se caracteriza por establecer objetivos específicos y ser muy estructurado, para abordar los escenarios planificados previamente a los que responderán los participantes.

Orden del día y horario: ejercicio de simulación de 90 minutos

01	**Bienvenida y presentaciones**	<5 minutos de tiempo>
02	**Objetivos y reglas del ejercicio**	<5 minutos de tiempo>
03	**Preparación del ejercicio**	<5 minutos de tiempo>
04	**Ejercicio basado en escenarios**	<60 minutos de tiempo>
05	**Reflexión en grupo/Lecciones aprendidas**	<15 minutos de tiempo>

Fuente: Gartner

Desarrolla un escenario y situaciones de incidentes

Los ejercicios de simulación ante incidentes de ciberseguridad son más eficaces si se estructuran como un escenario inicial (p. ej., malware), seguido de una serie de situaciones que aportan nueva información sobre el incidente ante el que los participantes deben reaccionar. Esta estructura reproduce la incertidumbre y la evolución de los contextos de incidentes reales.

	Tiempo transcurrido en la realidad: 5 horas	Tiempo transcurrido en el ejercicio: 60 minutos
Situación n.º 0: escenario inicial	8:00 h	10 minutos
Situación n.º 1: T + 30 minutos	8:30 h	10 minutos
Situación n.º 2: T + 1 hora	9:00 h	15 minutos
Situación n.º 3: T + 3 horas	11:00 h	5 minutos
Situación n.º 4: T + 4 horas	12:00 h	8 minutos
Situación n.º 4: T + 4,5 horas	12:30 h	7 minutos

Fuente: Gartner

Crea situaciones de incidentes desafiantes

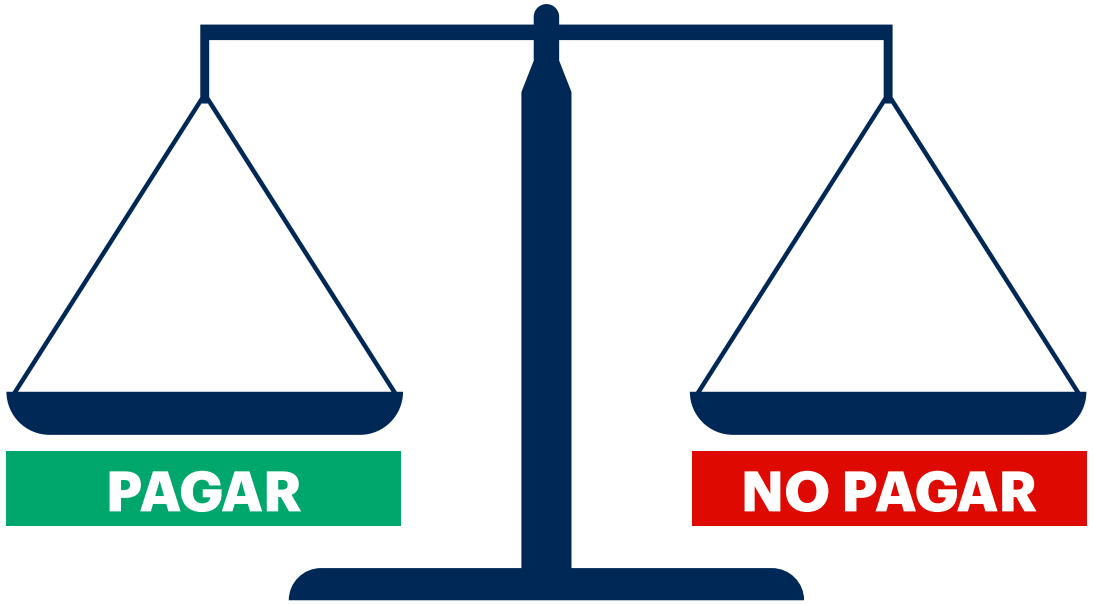
Los ejercicios de simulación de respuesta deben reproducir situaciones desafiantes que las partes interesadas deberán abordar durante un ataque real.

Ejemplo: Ransomware
En un ejercicio de simulación, puedes plantear a los participantes cómo reaccionarían a las exigencias de un atacante de ransomware.

Aspectos que debes tener en cuenta

Estos son algunos datos reales sobre el pago de rescates:

- Los archivos cifrados suelen ser irrecuperables.
- Las herramientas de descifrado que proporciona el atacante pueden bloquearse o no funcionar.
- La recuperación de los datos puede llevar mucho tiempo.
- No hay garantía de que los piratas informáticos eliminen los datos robados. Podrían vender o divulgar la información más adelante si tiene valor.
- A veces puede ser más fácil y económico pagar el rescate que intentar recuperar la copia de seguridad, aunque esta práctica, a su vez, fomenta el comportamiento delictivo.
- En algunos casos, pagar el rescate puede ser incluso ilegal.



Fuente: Gartner

Información práctica y objetiva

Descubre estos recursos y herramientas complementarios para responsables de seguridad y riesgos:

Hoja de ruta

Hoja de ruta de TI para la ciberseguridad

Crea una estrategia de ciberseguridad resiliente, ampliable y ágil.

Descargar ahora

Producto

Cómo colabora Gartner con los CISO

Descubre cómo Gartner ofrece recursos a los CISO y a sus equipos basados en información, orientación y herramientas.

Más información

Webinar

Las tendencias y tecnologías emergentes en seguridad de Gartner para 2024

Descubre las últimas tendencias y su impacto en las estrategias de seguridad y la dinámica del mercado.

Ver ahora

Ebook

4 maneras de lograr el comportamiento seguro de los empleados

Gestiona el riesgo humano y crea una organización concienciada con la seguridad.

Descarga el ebook

¿Ya eres cliente?
Obtén acceso a más recursos en tu portal de cliente. Iniciar sesión

Conecta con nosotros

Obtén conocimientos prácticos y objetivos que permitan una toma de decisiones más acertada y un mejor desempeño a la hora de abordar las principales prioridades estratégicas. Contacta con nosotros para hacerte cliente:

EE. UU.: +1 866 263 8917

Internacional: +44 (0) 3301 628 476

Hazte cliente

Obtén más información sobre Gartner para responsables de ciberseguridad
gartner.com/en/cybersecurity

Recibe las últimas novedades

Gartner